REMARKS

The Examiner is thanked for the performance of a thorough search.

SPECIFICATION

In the specification, the Abstract as originally filed has been replaced with a new Abstract. The Abstract as originally filed was objected to in the Office Action for exceeding the 150-word limit. Because the new Abstract does not exceed the 150-word limit, the Applicant respectfully submits that the objection to the Abstract has been traversed.

STATUS OF CLAIMS

Claims 3, 5, 7-9, 11, 13-14, 17-19, 21-22, 25-30, 32-33, 35-37, 39-41, 43-46, 49-50, 52-53, and 57-58 have been cancelled.

Claims 1, 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, and 54-56 have been amended.

Claims 59-101 have been added.

No claims have been withdrawn.

Claims 1, 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, and 59-101 are currently pending in the application.

SUMMARY OF THE REJECTIONS OF THE CLAIMS

Claims 1, 2, 4-6, 9-32, 34, 35, and 38-58 have been rejected under 35 U.S.C. § 102(b) as allegedly anticipated by U.S. Patent Number 6,240,188 issued to Dondeti et al. (" *Dondeti* "). Claim 3 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Dondeti* in view of U.S. Patent Number 6,570,847 issued to Hosein (" *Hosein* "). Claims 7, 33, and 36 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Dondeti* in view of U.S. Patent Number 6,247,014 issued to Ladwig et al. (" *Ladwig* "). Claim 8 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Dondeti* in view of U.S. Patent Number 6,240,188 issued to Newton Telecom Dictionary (" *Newton* "). Claim 37 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Dondeti* in view of U.S. Patent Number 6,240,513 issued to Friedman et al. (" *Friedman* "). The rejections are respectfully traversed.

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

As amended above, Claim 1 features:

"A method of establishing a secure communication session among a plurality of member nodes that participate in a multicast group across a wide area network, comprising the steps of:

receiving information defining a **plurality of multicast proxy service nodes**, wherein:

the plurality of multicast service nodes are distributed across the wide area network;

the **plurality of multicast service nodes** ***control when any of the*** **plurality of member nodes** ***join or leave the multicast group***; and

the plurality of multicast proxy service nodes are logically represented by a ***first*** **binary tree**, wherein:

each node of the ***first*** **binary tree** is associated with a ***domain of a plurality of domains of a directory service*** that is distributed across the wide area network; and

each node of the ***first*** **binary tree** is associated with one or more multicast proxy service nodes of the plurality of multicast proxy service nodes;

creating and storing a ***second*** **binary tree** that represents the plurality of member nodes, wherein:

each of the **member nodes** of the plurality of member nodes is represented by a leaf node of the ***second*** **binary tree**;

the ***second*** **binary tree** is stored in a ***particular domain of the plurality of domains of the directory service*** that is distributed across the wide area network;

a **root node** of the ***second*** **binary tree** represents **one or more of the multicast proxy service nodes** of the plurality of multicast proxy service nodes; and

each of the member nodes of the plurality of member nodes is capable of establishing multicast communication and serving as a key distribution center;

creating and storing a group session key associated with the multicast group and a private key associated with each member node of the multicast group using secure key exchange;

when an additional member node joins the multicast group, determining a new group session key by replicating a branch of the ***second*** **binary tree**." (Emphasis added.)

Thus, Claim 1 features two types of nodes: (1) **multicast proxy service nodes** and (2) **member nodes**. The multicast proxy service nodes control when the member nodes join or leave the multicast group, such as by functioning as group controllers, while the member nodes are capable of establishing multicast communication and serving as key distribution centers. Note that as defined in the Application, the term "multicast proxy service node" refers to a multicast service agent, multicast KDC, and/or a group controller. (Application, page 9, lines 6-7.)

Claim 1 also features two binary trees: (1) a ***first*** **binary tree** and (2) a ***second*** **binary tree**. The first binary tree logically represents the multicast proxy service nodes and each node of the first binary tree is associated with a domain of a plurality of domains of a directory service. The second binary tree represents the plurality of member nodes and is stored in a particular domain of the plurality of domains. The root node of the second binary tree represents one or more of the multicast proxy service nodes.

The amendments to Claim 1 are fully supported by the Application, and no new matter is introduced. For example, the embodiment illustrated by Figure 10A of the Application is of multicast group controllers that are distributed over a WAN using a binary tree approach. (Application, page 41, lines 6-9 and 19-21). A plurality of domains represented by domains 1004A, 1004B, 1004C, and 1004D for a directory service that are arranged according to a binary tree (e.g., a tree in which each parent node has two child nodes). (Application, page 41, lines 10-18.) Thus, the binary tree organization of domains 1004A, 1004B, 1004C, and 1004D is an example of the first binary tree in the approach of Claim 1.

Within each of domains 1004A, 1004B, 1004C, and 1004D are additional binary trees 1006A, 1006B, 1006C, and 1006D, each of which represents members of the multicast group that are within that domain. For example, in binary tree 1006A, there is a root node 1008, one or more intermediate nodes 1010, and one or more leaf nodes 10012. (Application, page 41, line 22 – page 42, line 7.) Thus, binary trees 1006A, 1006B, 1006C, and 1006D are examples of the second binary tree in the approach of Claim 1. Note that in Claim 1, there is only one second binary tree, whereas in the embodiment illustrated in Figure 10A, there are four examples of the second binary tree of the approach of Claim 1.

(2) INTRODUCTORY DISCUSSION OF *DONDETI*

In contrast to the approach of Claim 1, *Dondeti* discloses a group key management scheme utilizing a binary distribution tree structure of the members for providing secure many-to-many communications. (Abstract.) As described in the Background section of *Dondeti*, prior many-to-many group communication protocols all use centralized group control and thus are prone to a single failure and single point of attack. (Col. 1, lines 58-61.) Thus, *Dondeti's* approach is directed to decentralizing control of the group so that access control, key distribution, and dynamic group management tasks are delegate to all the sending members of the group. (Col. 1, lines 47-57.) In particular, *Dondeti* describes the main goal to be achieved by his new invention as that the group remains operational as long as one sender is operational by distributing access control and dynamic group management tasks to all senders, thereby allowing joins and leaves to be processed locally by the senders. (Col. 2, lines 19-33.) *Dondeti* contrasts his approach with those of the prior art that use centralized control, such as through the use of a group security controller. (Col. 1, lines 61-65.)

Therefore, *Dondeti's* approach can be described as one of decentralizing the conventional group security controller approach by moving access control and other management functions of the group from the central group controller to a collaborative approach in which access control and group management are handled by the members of the group, specifically the sending members of the group (in contrast to the receiving members of the group). As a result, *Dondeti* teaches away from the use of such centralized forms of group management, such as the use of a group security controller.

This is a fundamental difference between the approach of *Dondeti* and that of Claim 1 because in Claim 1, some centralized control is retained for controlling when members join or

leave the multicast group in the form of a plurality of multicast proxy service nodes, while control for key distribution is distributed to the group members that can act as key distribution centers. Thus, while Claim 1 and *Dondeti* are similar in that group members handle key distribution, Claim 1 differs from *Dondeti* in that control of members joining and leaving the group is retained by the multicast proxy service nodes.

Note that Claim 1 avoids the problem of centralized control cited by *Dondeti* (e.g., having a single point of failure or attack as with a single group security controller) by using multiple multicast proxy service nodes, so that the loss of one multicast proxy service node does not disable control of members joining or leaving the multicast group (e.g., the access control as described by *Dondeti* that is also distributed among the sending group members). Thus, the approach of Claim 1 retains centralized control over members joining and leaving the multicast group through the multiple multicast proxy service nodes, yet the approach of Claim 1 avoids the problems of centralized group control as described by *Dondeti* through the use of multiple multicast proxy service nodes.

Finally, note that in FIGs. 1, 2, 3, 4, and 9 of *Dondeti*, examples of binary tree arrangements of member nodes are illustrated. However, as described in *Dondeti*, each of these binary trees represents the group members as opposed to group controllers or other centralized group control entities. Thus, while *Dondeti* provides multiple examples of binary tree arrangements, all are similar in that the binary trees represent group members, not group controllers or any other type of multicast proxy service node.

(3) THE OFFICE ACTION'S CITATIONS FROM *DONDETI*

The Office Action states that *Dondeti* discloses, *inter alia*, "a plurality of multicast proxy service nodes..., wherein the multicast proxy service nodes are logically represented by a first binary tree [column 3 line 58 to column 4 line 21]..." However, the cited portion of *Dondeti* actually describes a key distribution tree representing the ***members*** of the multicast group, **not multicast proxy service nodes** or some other type of group controller as in the first binary tree of Claim 1. (Col. 3, lines 48-49 and 64-65.) The balance of the cited portion describes how the group members control the group through the computation of the root key through the use of blinded and unblinded versions of each member's secret key. (Col. 3, lines 49-63 and Col. 4, lines 1-21.)

Furthermore, as amended above, Claim 1 features that the nodes of the first binary tree are associated with "a plurality of domains of a directory service," and the Applicant has been unable to find anything in either the cited portions of *Dondeti* or any other part of *Dondeti* that discloses a binary tree in which nodes are associated with domains of a directory service. Multiple searches of *Dondeti*, both by reading the patent and making electronic searches, have failed to disclose any occurrences of the words "directory" or "domain" or anything corresponding to either a directory or a domain, little less that multiple domains of a directory service are organized in a first binary tree, as in the approach of Claim 1.

The Office Action also states that *Dondeti* discloses, *inter alia*, "creating and storing a second binary tree for representing the member nodes, wherein each of the member nodes is represented by a leaf node of the second binary tree, that is stored in a domain of a directory service...[column 3 line 58 to column 4 line 21]..." Note that this is the same citation that the Office Action alleges as disclosing the first binary tree. Yet while this cited portion of *Dondeti* does describe a binary tree arrangement of member nodes, there is nothing in this cited portion of *Dondeti* or elsewhere that the described binary tree representation is stored in a domain of a directory service, as in the approach of Claim 1.

Furthermore, as amended herein, Claim 1 features that "a root node of the second binary tree represents one or more of the multicast proxy service nodes," which control the members that join and leave the group. As discussed above, *Dondeti* clearly teaches away from the use of such centralized group access control by having the sending member nodes perform such functions, and thus the Applicant fails to see how any of the disclosure of *Dondeti* can be reasonably interpreted as disclosing that the root nodes of *Dondeti's* binary tree correspond to one or more multicast proxy service nodes, such as one or more group controllers, since it is the aim of *Dondeti* to not use such centralized group control.

Thus, while *Dondeti* discloses a binary tree arrangement of member nodes, group control, including both key distribution and access control, is shared among the sending member nodes, and thus *Dondeti* does not use group controllers or any other type of multicast proxy service node. In contrast, the approach of Claim 1 retains centralized control of members joining and leaving the group through the use of multiple multicast proxy service nodes. Furthermore, the multicast proxy service nodes are represented by another binary tree besides the binary tree that represents the members, and the nodes of the binary tree are associated with domains of a directory service, yet *Dondeti* fails to disclose anything like this

other binary tree of Claim 1, little less that such a binary tree has nodes associated with multiple domains of a directory service.

(4) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *DONDETI*

Because *Dondeti* fails to disclose, teach, suggest, or in any way render obvious that "the multicast proxy service nodes are logically represented by a first binary tree," that "the plurality of multicast proxy service nodes control when any of the plurality of member nodes join or leave the multicast group," that "each node of the first binary tree is associated with a domain of a plurality of domains of a directory service," that "each node of the first binary tree is associated with one or more multicast proxy service nodes" and " a second binary tree that represents the plurality of member nodes" in which "a root node of the second binary tree represents one or more of the multicast proxy service nodes," the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

C. CLAIMS 59, 60, AND 81

Claims 59, 60, and 81 contain features that are that same as those described above with respect to Claim 1, and all feature "the multicast proxy service nodes are logically represented by a first binary tree," that "the plurality of multicast proxy service nodes control when any of the plurality of member nodes join or leave the multicast group," that "each node of the first binary tree is associated with a domain of a plurality of domains of a directory service," that "each node of the first binary tree is associated with one or more multicast proxy service nodes" and " a second binary tree that represents the plurality of member nodes" in which "a root node of the second binary tree represents one or more of the multicast proxy service nodes," as in Claim 1. Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 59, 60, and 81 are allowable over the art of record and are in condition for allowance.

D. CLAIMS 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 61-80, AND 82-101

Claims 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, and 54-56 are dependent on Claim 1, Claims 61-80 are dependent on Claim 60, and Claims 82-101 are

dependent upon Claim 81. Each of Claims 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 61-80, and 82-101 is therefore allowable for the reasons given above for Claims 1, 60, and 81. In addition, each of Claims 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 61-80, and 82-101 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of most of those limitations is not included at this time, except for the dependent claims that are addressed below. Therefore, it is respectfully submitted that Claims 2, 4, 6, 10, 12, 15-16, 20, 23-24, 31, 34, 38, 42, 47-48, 51, 54-56, 61-80, and 82-101 are allowable for the reasons given above with respect to Claims 1, 60, and 81.

(1) CLAIMS 2, 61, AND 82

Claims 2, 61, and 82 each feature "***joining* an additional group controller** to the plurality of group controllers, wherein each group controller of the plurality of group controllers is a **replica** of another group controller of the plurality of group controllers" and "receiving a request to add or delete a specified member node of the multicast group from a **load balancer** that is coupled to the plurality of group controllers." The Office Action states that *Dondeti* discloses "wherein each of the multicast proxy service nodes acts as one of a plurality of replicated group controllers," although no citation to *Dondeti* is provided in the Office Action. However, the Office Action provides the same citation for all the steps of Claim 2, namely "[column 6 line 22 to column 8 line 42]," so the Applicant will proceed on the assumption that that citation applies to the above feature of Claims 2, 61, and 82.

The two columns of material from *Dondeti* that are cited in the Office Action for Claim 2 describe a "Join Protocol Procedure #1," a "Join Protocol Procedure #2," and "Synchronized Joins." Yet in none of these sections of *Dondeti*, nor any other portion of *Dondeti*, is the Applicant able to identify any group controllers, little less a plurality of group controllers, little less that each group controller of the plurality of group controllers is a replica of another group controller. As discussed above, *Dondeti* teaches away from the use of a group controller and instead has group management functions handled by the group members themselves instead of a group controller.

Furthermore, the Applicant is unable to identify anything that is replicated in the join procedures described in *Dondeti*. While these sections describe that member node C splits its

ID 010, resulting members C and J are cannot be replicas of each other since each has its own unique key (e.g., 0100 for C and 0101 for J). In fact, as illustrated in FIGs 2, 3, 4, and 9, each member is different and has a unique key, and therefore none of the members can be replicas of each other, little less be considered group controllers that are replicas of another group controller, as in Claims 2, 61, and 82.

In addition, the Applicant has been unable to locate within the cited portion of *Dondeti* or elsewhere any disclosure of a load balancer, little less that a request is received from a load balancer to add or delete a specified member of the multicast group. While the first join procedure states that "it is desirable to control at which node a prospective member joins in order to keep the key tree balanced" (Col. 6, lines 22-25), keeping the tree "balanced" is not the same as a load balancer from which a request is received to join a member. As best understood by the Applicant, in the join procedures, the original of the join is only described as coming from a request of the new member that wants to join (Col. 7, lines 43-45), and thus the request is not from a load balancer as in the approach of Claims 2, 61, and 82.

Because *Dondeti* fails to disclose, teach, suggest, or in any way render obvious that "joining an additional group controller to the plurality of group controllers, wherein each group controller of the plurality of group controllers is a replica of another group controller of the plurality of group controllers" and "receiving a request to add or delete a specified member node of the multicast group from a load balancer that is coupled to the plurality of group controllers," the Applicant respectfully submits that, for at least the reasons stated above, Claims 2, 61, and 82 are allowable over the art of record and is in condition for allowance.

(2) CLAIMS 12, 65, AND 86

Claims 12, 65, and 86 each feature "communicating the collective public key" by "determining whether the first member node or the second member node transfers the collective public key based upon an order of entry of the first and second member nodes into the multicast group." The Office Action states that *Dondeti* discloses "communicating the collective public key further comprises determining whether the first member node or the second member node transfers the collective public key based upon an order of entry of such member nodes into the multicast group [column 6 line 43 to column 7 line 13]." However, the Applicant is unable to find in the cited portion of *Dondeti* or elsewhere making a

determination of which member node distributes a collective public key between two member nodes as in Claims 12, 65, and 86, little less that such a determination is based on the order of entry of the two member nodes between which the determination is made.

Furthermore, the Applicant is unable to locate anything within the cited portion of *Dondeti* that corresponds to a collective public key. Rather, the cited portion of *Dondeti* describes the sharing of blinded versions of each nodes secret key, from each node then computes the root key, and thus there is nothing corresponding to a collective public key as in Claims 12, 65, and 86.

(3) CLAIMS 15, 66, AND 87

Claims 15, 66, and 87 each feature "computing and storing a group shared secret key value "k" at the first member node according to the relation:

$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$;

wherein:"

"a is the first private value of the first member node,

"b is the second private value of the second member node,

"c is the third private value of the third member node,"

Note that in Claims 15, 66, and 87, it is the private keys of the three member nodes that are used to compute the group shared secret key.

The Office Action cites "[column 4, lines 49-65]" of *Dondeti* as disclosing these features of Claim 15. However, the cited portion of *Dondeti* only describes that the group members exchange "***blinded*** versions 30 of their secret keys 28 with each other." (Col. 4, lines 53-55; emphasis added.) But the blinded versions of the secret keys are merely "computed by applying a given one-way function to the secret key. Given a blinded key that is calculated with a one-way function, it is computationally infeasible to compute the unblinded counterpart of the blinded key." (Col. 4, lines 7-11.) As best understood by the Applicant, the "private keys" in Claims 15, 66, and 87 correspond to the "secret keys" of *Dondeti*. Yet in *Dondeti*, the group members do not exchange their private keys and cannot determine each other's private keys based on the blinded keys since such an effort is "computationally infeasible" according to *Dondeti*, and thus the group members are unable to compute the group shared secret key value "k" by the relation given above.

(4) CLAIMS 16, 67, AND 88

Claims 16, 67, and 88 each feature "creating and storing information at the first member node..., wherein the collective public key is based on the first private key and a second private key that is derived by the first member node from the second public key." The Office Action cites "[column 8, lines 16-42]" of *Dondeti*, which merely describes synchronized joins using either version numbers for internal keys and mixing functions for some or all occasions. Yet there is nothing in the cited portion about the first member node deriving the private key of a second member node from the second member nodes public key. In fact, as described above, since the members only exchange blinded keys that are computed by applying one-way hash functions to each member's secret key, it is not clear to the Applicant how one member node could determine the secret key of another member node with *Dondeti's* approach.

(4) CLAIMS 20, 68, AND 89

Claims 20, 68, and 89 are similar to Claims 12, 65, and 86 discussed above in that a "shared secret key value, k," is computed based on the three private keys of three member nodes. The Office Action cites the same portion of *Dondeti* as with Claims 12, 65, and 86, and therefore the Applicant respectfully submits that Claims 20, 68, and 89 are allowable over the cited prior art for the same reasons given above for Claims 12, 65, and 86.

(5) CLAIMS 24, 38, 70, 73, 91, AND 94

Claims 24, 38, 70, 73, 91, and 94 each feature both a "directory system agent" and a "replication service agent" that are associated with a multicast proxy service node. The Office Action cites "[column 10 line 61 to column 11 line 36]" in the rejections of Claims 25 and 39 that originally included these features now incorporated into Claims 24, 38, 70, 73, 91, and 94. However, the cited portion of *Dondeti* describes "Subgroups" and "Few-to-many Group Formation," neither of which discloses either a directory system agent (DSA)or a replication service agent (RSA). And as described above, *Dondeti* teaches away from centralized group control, such as through the use of group controllers or other multicast proxy service nodes, and thus, even if there were something in *Dondeti* corresponding to either a DSA or an RSA, neither would be part of a multicast proxy service node, as in Claims 24, 38, 70, 73, 91 and 94.

(5) CLAIMS 24, 42, 56, 70, 74, 80, 91, 95, AND 101

Claims 24, 42, 56, 70, 74, 80, 91, 95, and 101 each feature "replicating the directory" in which "key information," "group session key information," or a "group session key" is stored in the directory. The Office Action cites "[column 10 line 61 to column 11 line 36]" as disclosing "replicating the directory" in rejecting Claims 28 and 43, the features of which are now incorporated into Claims 24 and 42 and "[column 4, lines 29-63]" in rejecting Claim 56. Yet as discussed above, the Applicant is unable to find any occurrence of the word "directory" or any disclosure of anything akin to a directory within either the cited portions of *Dondeti* or any other portion of *Dondeti*.

Specifically, in the first cited portion of *Dondeti*, a description of Subgroups is provided with reference to FIG. 9, but that section says nothing about a directory, little less the replication of a directory in which is stored key or key information. The first cited portion of *Dondeti* also describes few-to-many group formation in which receivers must send data via a sender in the receivers subgroup that is also in the senders group, but that again says nothing about replicating a directory that stores key or key information. Finally, the second cited portion of *Dondeti* describes the exchange of blinded versions of keys among members and the finding of neighbor members with which to exchange keys, but that again says nothing about a directory, little less replicating such a directory in which is stored key or key information.

(6) CLAIMS 47, 54, 75, 78, 96, AND 99

Claims 47, 54, 75, 78, 96, and 99 each feature "securely communicating the group session key using a secure back channel." The Office Action cites *Dondeti* "[column 10 line 29 to column 11 line 14]" in rejecting this feature of Claim 47 and "[column 5 line 53 to column 6 line 4]" in rejecting this feature of Claim 54. However, the first cited portion of *Dondeti* is yet another reference to the Subgroup discussion, in which *Dondeti* states that members of a subgroup can communicate with other members of the subgroup using a common group root key for the subgroup, but nowhere does this section describe that such a common group root key via a secure back channel. Similarly, the second cited portion of *Dondeti* describes how each member compute the root key for the group, but again, this is performed via the blinded keys of each member that are exchanged, and there is nothing about using a secure back channel for the communication of the root key.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: December 28, 2005

Craig G. Holmes
Reg. No. 44,770

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop AMENDMENT, P.O. Box 1450, Alexandria, VA 22313-1450.

on 12/28/05 by